INFORMATION AND CONTROL 48, 193–210 (1981)

Spectral Enumerators for Certain Additive-Error-Correcting Codes over Integer Alphabets

PH. DELSARTE AND PH. PIRET

Philips Research Laboratory, Brussels, Belgium

The paper contains a study of certain block codes, with integer coordinate symbols, devised for the correction of some types of additive errors. The codes are defined by a check equation over a finite Abelian group; thus they appear as an extension of the Varshamov and Constantin–Rao codes. The main results of the paper are concerned with the error-correcting capability, including a decoding method for generalized Varshamov codes, and principally with enumeration problems. A general formula for spectral enumerators is obtained and applied to the Varshamov and Constantin–Rao codes.

1. INTRODUCTION

The aim of this paper is to investigate certain classes of block codes, defined over *integer alphabets*, that allow correction of certain *additive errors*. A typical code C consists of the n-tuples $\mathbf{v}$, with coordinate symbols v_i in the given alphabet, that satisfy a *check equation* of the form $v_1h_1 + v_2h_2 + \cdots + v_nh_n = h_0$, where the h_i's are fixed elements of a finite Abelian group. Let s be the period of this group. In the special case where the aphabet is the interval $[0, s-1]$ it appears that C is a *coset* of an s-ary *group code*. On the other hand, it turns out that the general code C (defined over any integer alphabet) can be deduced in a straightforward manner from the special code just mentioned. In particular, when the alphabet is finite, the cardinality of C is directly computable from the *spectral enumerator* of the special code.

Our main interest is in those codes C that correct all additive errors $\mathbf{e}$, with coordinates e_i in $[0, s-1]$, the *amplitude* $e_1 + \cdots + e_n$ of which is less than or equal to a given integer t. Codes having this error-correcting capability are called *t-codes* in the present paper. The 1-codes first constructed by Varshamov and Tenenholtz (1965) were generalized by Stanley and Yoder (1973) who considered the whole class of maximum length 1-codes over an interval alphabet $[0, c-1]$. The same class was recently rediscovered and studied in detail by Constantin and Rao (1979) in the binary case ($c = 2$). The cardinality of the binary Varshamov–Tenenholtz codes was obtained by Ginzburg (1967) and that of the Constantin–Rao

0019-9958/81/030193–18$02.00/0

codes by McEliece and Rodemich (1980). The weight distribution of the Varshamov–Tenenholz codes was determined by Mazur (1974) in the binary case and by Stanley and Yoder (1973) in the general c-ary case. The cardinality and the weight distribution of the c-ary Stanley–Yoder codes (which reduce to the Constantin–Rao codes in the binary case) were recently obtained by Helleseth and Kløve (1981).

Varshamov (1973) discovered a remarkable class of c-ary t-codes with $t \geqslant 1$, which are closely related to classical *BCH* codes over prime fields. Varshamov's codes were further investigated by McEliece (1973), who gave a simple proof of their error-correcting capability and mentioned a useful average bound on their cardinality. Mazur (1974) showed that the cardinality of a given code is relatively close to this average value. An interesting decoding method for the binary Varshamov codes was proposed by Nalbandyan (1974).

In the present paper certain generalizations of the codes quoted above are studied in detail, both from the viewpoint of *error correction* and of *enumeration*. The paper is organized as follows.

Section 2 first gives a brief algebraic description of the type of errors that our codes are required to correct. Then the definition of the codes is given, in terms of a check $(n+1)$-tuple over an Abelian group. An elementary theorem establishes a link between these two concepts. Thereafter, generalized versions of Constantin–Rao codes and Varshamov codes are described. In particular, a theorem is given concerning the error-correcting capability of generalized Varshamov codes. The proof is an extension of that used by Nalbandyan (1974); it contains a decoding algorithm similar to that devised for *BCH* codes. An interesting consequence of this theorem is that p-ary *BCH* codes are able to correct more asymmetric errors than is guaranteed by the designed Hamming distance. Finally, constructions are mentioned of constant weight codes from binary asymmetric-error-correcting codes. This idea was first applied by Bose and Rao (1978) to derive certain codes with well-defined correcting and detecting properties from the Constantin–Rao codes. The same idea was implicitly used by Graham and Sloane (1980) who deduced interesting constant weight binary codes from a class of codes closely related to generalized Varshamov codes.

The subject of Section 3 is enumeration. After a preliminary result which generalizes the average bound given by McEliece (1973), the concept of the s-ary spectral enumerator of a code C is introduced. Our definition is directly inspired by that of "complete weight enumerator" in classical coding theory; see MacWilliams *et al.* (1972). In the important case of the binary alphabet $\{0, 1\}$, the spectral enumerator reduces to the Hamming weight enumerator. The main result, which potentially has a large field of application, is an explicit formula for the spectral enumerator of the code C in terms of the check $(n+1)$-tuple defining C. The ideas underlying the

proof go back to a paper by MacWilliams (1963). In fact, our formula can be viewed as a generalization of the MacWilliams identity for weight enumerators of dual codes. The rest of Section 3 is devoted to applying the general result to the weight enumerators of Constantin–Rao codes, on the one hand, and certain generalized Varshamov codes, on the other hand. For the first class of codes the outcome is a closed form expression of the weight enumerator in terms of elementary number and group theoretic functions; an equivalent expression was discovered and analysed in detail by Helleseth and Kløve (1981). The case of generalized Varshamov codes is much more difficult; the results given here are restricted to the class of binary 2-codes (of full length), for which explicit formulas are derived by use of the theory of quadratic residues. Several examples are mentioned throughout this section.

2. Error-Correcting Capability

Before defining our codes let us briefly explain to what kind of transmission channel they are adapted. The transmitted symbols are elements of a given subset A of $\mathbb{Z}$, called the *alphabet*, with $|A| \geqslant 2$, while the error symbols belong to the subset $S = \{0, 1,..., s-1\}$ of $\mathbb{Z}$ for a certain $s \geqslant 2$. Given an element e of S let A_e denote the subset of the alphabet A consisting of the symbols that can be affected by e. In case A_e is not empty, the effect of e is described by an injective mapping f_e from A_e into $\mathbb{Z}$ subject to the additivity condition $f_e(a) \equiv a + e \pmod{s}$ for all $a \in A_e$. Let us now mention three important particular cases, which provide the motivation of our study: (i) the strictly additive channel over the integers, with $A_e = A = \mathbb{Z}$ and $f_e(a) = a + e$; (ii) the classical s-ary channel, with $A_e = A = S$ and $f_e(a) =$ residue of $a + e$ modulo s; (iii) the asymmetric c-ary channel with $A = \{0, 1,..., c-1\}$, $A_e = \{0, 1,..., c-1-e\}$ and $f_e(a) = a + e$.

Let $(G, +, 0)$ be a *finite Abelian group*, or, equivalently, a finite module over the ring $\mathbb{Z}$. For a given integer $n \geqslant 2$, consider any n-tuple $\mathbf{h}(h_1, h_2,..., h_n)$ of elements $h_i \in G$. Without loss of generality we shall assume that the h_i's generate G. Define the code C, of length n over the alphabet A, to consist of the n-tuples that yield a fixed element $h_0 \in G$ when acting on $\mathbf{h}$ by linear combination. Formally,

$$C = \{\mathbf{v} \in A^n : \mathbf{v}\mathbf{h}^T = h_0\}, \tag{1}$$

where $\mathbf{v}\mathbf{h}^T$ denotes the "scalar product" $v_1 h_1 + v_2 h_2 + \cdots + v_n h_n$ for $\mathbf{v} = (v_1, v_2,..., v_n)$. In the sequel $(h_0, \mathbf{h})$ will be referred to as the *check* $(n+1)$*-tuple* for the code C. The *period* of the group G will appear to be an important parameter; it is the smallest positive integer s satisfying $sh_i = 0$ for $i = 1, 2,..., n$.

Let us draw the attention of the reader to two topics about *isomorphisms* which lead to simplifications in the complete analysis of a family of codes (1). Consider an automorphism σ of the group G that permutes the elements $h_1, h_2, \ldots, h_n$. Then replacing h_0 by $\sigma(h_0)$ yields a code which is permutation-equivalent to the original code C. On the other hand, assume the alphabet A is symmetric with respect to a certain integer r, in the sense that $r-a$ belongs to A for all $a \in A$. Then replacing h_0 by $r(h_1 + \cdots + h_n) - h_0$ transforms C into its r-complement (where any symbol v_i is replaced by $r - v_i$). An example is provided by the binary alphabet $A = \{0, 1\}$ with $r = 1$.

When necessary, the notation C_A will be used for the code (1) over the given alphabet A. Let $S = \{0, 1, \ldots, s-1\}$, where s is the period of G. The code C_S is naturally associated with the group G and plays a special role in the theory. It appears indeed that, for a given check $(n+1)$-tuple $(h_0, \mathbf{h})$, any code C_A can be immediately deduced from C_S: the code C_A consists of the vectors congruent modulo s to the vectors of C. Formally,

$$C_A = \bigcup_{\mathbf{u} \in C_S} \{\mathbf{v} \in A^n : v_i \equiv u_i \pmod{s}, \text{ all } i\}. \tag{2}$$

Of course, in case A is a subset of S one simply has $C_A = A^n \cap C_S$. It is also important to observe that, if S is viewed as the cyclic group of order s, then C_S has the structure of a *coset of a group code* over S.

As a first result, let us give a simple characterization of the error-correcting capability of the code $C = C_A$, for any alphabet A.

THEOREM 1. *Let $S = \{0, 1, \ldots, s-1\}$ where s is the period of G. Let E be a subset of S^n having the property that the elements $\mathbf{e}\mathbf{h}^T$ of G are distinct when $\mathbf{e}$ varies over E. Then the code C with check $(n+1)$-tuple $(h_0, \mathbf{h})$ is capable of correcting all errors belonging to E.*

Proof. Let $\mathbf{v}$ be any transmitted codeword; by definition $\mathbf{v}\mathbf{h}^T = h_0$. The error vector $\mathbf{e} \in E$ and the received vector $\mathbf{x} \in \mathbb{Z}^n$ are related by $x_i \equiv v_i + e_i \pmod{s}$. Hence the "syndrome" $b = \mathbf{x}\mathbf{h}^T - h_0$ equals $\mathbf{e}\mathbf{h}^T$. Now, by assumption, there is a unique $\mathbf{e} \in E$ satisfying $\mathbf{e}\mathbf{h}^T = b$. This shows that $\mathbf{e}$, hence $\mathbf{v}$, can be uniquely determined from the received vector, which proves the assertion. ∎

The *amplitude* $\|\mathbf{x}\|$ of a vector $\mathbf{x} \in \mathbb{Z}^n$ is defined to be its l_1-norm, i.e., $\|\mathbf{x}\| = |x_1| + |x_2| + \cdots + |x_n|$. In this paper we are mainly interested in codes that correct all errors of amplitude less than or equal to a given integer t; these codes will be referred to as *t-codes*. To apply Theorem 1 in this case it suffices to put $E = \{\mathbf{e} \in S^n : \|\mathbf{e}\| \leqslant t\}$.

Maximum length 1-codes are easily identified. A typical code C of this class is defined as in (1) from a check $(n+1)$-tuple $(h_0, \mathbf{h})$, where $h_1, h_2, \ldots, h_n$ are the distinct nonzero elements of a given Abelian group G (of

order $n+1$) and h_0 is any element of G. (See Stanley and Yoder (1973), and Constantin and Rao (1979).) It is immediate from Theorem 1 that C actually is a 1-code, for any additive channel as described above. Moreover it appears that all t-codes with $t \geqslant 1$ can be obtained by shortening a maximum length 1-code. (Exactly as, in classical coding theory, all linear codes with minimum distance $\geqslant 3$ can be viewed as shortened Hamming codes.)

The construction of t-codes with $t \geqslant 2$ is not so obvious. We shall now describe an important family of such codes, the discovery of which should be essentially attributed to Varshamov (1973). Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ denote n distinct nonzero elements of the Galois field $F = GF(p^m)$, with p a prime number and m a positive integer. Construct the $t \times n$ matrix

$$H = \begin{bmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & & \vdots \\ \alpha_1^t & \alpha_2^t & \cdots & \alpha_n^t \end{bmatrix}, \tag{3}$$

for a given $t \geqslant 1$. Furthermore, let $\boldsymbol{\lambda} = (\lambda_1, \lambda_2, \ldots, \lambda_t)$ denote any t-tuple of elements $\lambda_k \in F$. Then the *generalized Varshamov code* C is defined to be the set of n-tuples $\mathbf{v}$ over the alphabet A satisfying $\mathbf{v}H^T = \boldsymbol{\lambda}$. (Varshamov considered the case $m = 1$.) These codes clearly belong to the general framework (1); the appropriate group G is the additive group of F^t (i.e., the elementary Abelian p-group of order p^{mt}), and the check $(n+1)$-tuple is the matrix $(\boldsymbol{\lambda}^T, H)$ where the columns are viewed as elements of G. Note that $s = p$.

THEOREM 2. *The generalized Varshamov code with check matrix* $(\boldsymbol{\lambda}^T, H)$ *is a* t*-code provided* t *does not exceed* $p-1$.

Proof. The argument presented here directly leads to a decoding algorithm. It is obviously inspired by the classical approach to *BCH* codes and related codes; see especially Berlekamp (1968) in that respect. As defined in the proof of Theorem 1, the syndrome relative to the error vector $\mathbf{e}$ is the vector $(\beta_1, \ldots, \beta_t)^T$ given by

$$\beta_k = \sum_{i=1}^{n} e_i \alpha_i^k, \qquad k = 1, \ldots, t. \tag{4}$$

Thus β_k is the kth power moment of the multiset in which α_i occurs e_i times $(i = 1, \ldots, n)$. Next, let σ_j denote the jth elementary symmetric function defined over the same multiset. Thus, putting $w = \|\mathbf{e}\|$ and assuming $w \leqslant t$, one has the identity

$$\sum_{j=1}^{t} (-1)^j \sigma_j z^{t-j} = z^{t-w} \prod_{i=1}^{n} (z - \alpha_i)^{e_i}. \tag{5}$$

(Note that σ_j vanishes for $j > w$.) Now $\sigma_1, \sigma_2, \ldots, \sigma_t$ can be calculated from the components (4) of the syndrome via Newton's identities. Finally, the integers e_i are uniquely determined from factorizing the polynomial $\sigma(z)$ in the left member of (5). Thus we have shown that all errors $\mathbf{e}$ of amplitude $\|\mathbf{e}\| \leqslant t$ are correctable, and we have sketched a decoding method. ∎

Let us now emphasize an interesting application of Theorem 2, in the classical case $A = S = \{0, 1, \ldots, p-1\}$ with $f_e(a) =$ residue of $a + e \pmod p$ for a and e in S. In this situation the generalized Varshamov code C is a coset of a shortened *BCH* code over $GF(p)$ with designed Hamming distance $t+1$. Hence C is capable of correcting all errors of Hamming weight not exceeding $t/2$. Theorem 2 says that C can be used to correct other types of errors, namely those of amplitude not exceeding t. For example, let $p = 3$ and $t = 2$; the algorithm described above corrects all simple errors and, in addition, all double errors with nonzero coordinates equal to 1.

In case the alphabet A is a subset of the error set $S = \{0, 1, \ldots, s-1\}$ and the error function $f_e(a)$ is the integer addition $a + e$, a noteworthy interpretation of t-codes can be given in the framework of metric spaces. To that end let us consider the natural generalization of the asymmetric minimum distance introduced by Rao and Chawla (1975) for binary codes. Given two n-tuples $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_n)$ with integer coordinates x_i, y_i, the asymmetric distance $d(\mathbf{x}, \mathbf{y})$ is defined to be

$$d(\mathbf{x}, \mathbf{y}) = \max \left\{ \sum_{x_i \leqslant y_i} (y_i - x_i), \sum_{y_i \leqslant x_i} (x_i - y_i) \right\}, \tag{6}$$

which actually enjoys the properties of a metric. Then the *minimum asymmetric distance* d_C of any code C over A is the minimum value assumed by $d(\mathbf{x}, \mathbf{y})$ over all pairs of distinct codewords $\mathbf{x}$ and $\mathbf{y}$ in C. The reader will easily convince himself that, in the present situation, t-codes C are exactly those having minimum asymmetric distance $d_C \geqslant t + 1$. This property of t-codes has the following consequence in the binary case, i.e., $A = \{0, 1\}$. The set D_k of all codewords of a fixed Hamming weight k in C has minimum Hamming distance $\geqslant 2d_C \geqslant 2t + 2$. Furthermore, adding an extra coordinate to the union of D_k and D_{k-1} yields a code Γ_k of length $n' = n + 1$ and constant weight k with minimum distance $\geqslant 2t + 2$. Certain results about this construction will be mentioned in the sequel. (See also Graham and Sloane (1980).)

3. Spectral Enumerators

Throughout this section, the alphabet A is assumed to be finite. The question considered here is the following: how to determine the cardinality, or, more generally, the spectral enumerator of the code C given by (1)? The

importance of knowing $|C|$ is quite obvious. Our motivation for computing spectral enumerators is mainly provided by the construction of constant weight binary codes mentioned in the end of Section 2. In addition, let us point out that the spectral enumerator of the code C_S directly yields the cardinality of C_A for any alphabet A.

Let us start with a preliminary result, which has been first mentioned by McEliece (1973) in the case of Varshamov codes.

THEOREM 3. *For any alphabet A and any n-tuple $\mathbf{h}$ over the group G, there exists an element $h_0 \in G$ such that the corresponding code* (1) *satisfies* $|C| \geqslant |A|^n |G|^{-1}$.

Proof. Let $C[h_0]$ denote the code (1). Since the collection of all nonempty codes $C[h_0]$ is a partition of A^n it appears that the average cardinality of $C[h_0]$ equals $|A^n||G|^{-1}$, which proves the theorem. ∎

In the case of the alphabet $A = S = \{0, 1,..., s-1\}$, with s the period of G, the codes $C[h_0]$ are cosets of the group code $C[0]$, so that all these codes have cardinality $s^n |G|^{-1}$. For a general alphabet A, the problem is much more complicated. We shall obtain an expression for the cardinality of C_A by use of the *Fourier transform*; our method is clearly inspired from the one introduced in a classical paper by MacWilliams (1963).

The s-ary *spectrum* of a vector $\mathbf{v} = (v_1, v_2,..., v_n) \in \mathbb{Z}^n$ is defined to be the s-tuple $c(\mathbf{v}) = (c_0(\mathbf{v}), c_1(\mathbf{v}),..., c_{s-1}(\mathbf{v}))$, where $c_k(\mathbf{v})$ counts the coordinate positions $i \in \{1,..., n\}$ such that $v_i \equiv k \pmod s$. Then the *spectral enumerator* of the code C is the polynomial $C(\mathbf{z}) = C(z_0, z_1,..., z_{s-1})$, homogeneous of degree n in the indeterminates z_k, in which the coefficient of the monomial

$$\mathbf{z}^{\boldsymbol{\tau}} = z_0^{\tau_0} z_1^{\tau_1} \cdots z_{s-1}^{\tau_{s-1}} \tag{7}$$

counts the codewords $\mathbf{v} \in C$ having spectrum $c(\mathbf{v}) = \boldsymbol{\tau} = (\tau_0, \tau_1,..., \tau_{s-1})$. Thus, with the notation (7), one can write

$$C(\mathbf{z}) = \sum_{\mathbf{v} \in C} \mathbf{z}^{c(\mathbf{v})}. \tag{8}$$

In particular, substituting $\mathbf{z} = \mathbf{1} = (1, 1,..., 1)$ in (8) yields $C(\mathbf{1}) = |C|$. In view of (2) the spectral enumerator of $C = C_A$ is readily deduced from that of C_S. Indeed, let $\boldsymbol{\theta} = (\theta_0, \theta_1,..., \theta_{s-1})$ be the s-ary spectrum of the alphabet A; by definition, θ_k counts the symbols $a \in A$ satisfying $a \equiv k \pmod s$. Then the spectral enumerator of C_A is given by the formula

$$C_A(\mathbf{z}) = C_S(\boldsymbol{\theta}\mathbf{z}), \tag{9}$$

where $\boldsymbol{\theta}\mathbf{z}$ stands for the componentwise product of the s-tuples $\boldsymbol{\theta}$ and $\mathbf{z}$. The proof of this result is elementary and left to the reader. (In fact, (9) immediately follows from the explicit expression derived below.) Specializing (9) to $\mathbf{z} = \mathbf{1}$ shows how the numerical values assumed by the spectral enumerator of C_S yield the cardinalities of all codes C: one has $C_S(\boldsymbol{\theta}) = |C_A|$ for any alphabet A of spectrum $\boldsymbol{\theta}$.

Let us particularly mention the binary case $A = \{0, 1\}$. Clearly, the spectral enumerator $C(\mathbf{z})$ depends only on z_0 and z_1. By abuse of notation we shall write $C(z) = C(1, z, *, \ldots, *)$. This polynomial $C(z)$ simply is the classical *weight enumerator* of the binary code C. It is obtained from the spectral enumerator of C_S by substituting $\boldsymbol{\theta} = (1, 1, 0, \ldots, 0)$ in (9).

It will prove useful to dispose of a matrix representation of the check $(n+1)$-tuple $(h_0, \mathbf{h})$. To that end, let us consider the canonical representation of the group G as the direct product of its *invariant factors* $G^{(k)}$; see, e.g., Curtis and Reiner (1962). There exists uniquely determined integers $s_1, s_2, \ldots, s_r$, with $s_k \geqslant 2$ for all k, satisfying the divisibility condition $s_k \mid s_{k-1}$, such that one has the isomorphism

$$G \cong G^{(1)} \times G^{(2)} \times \cdots \times G^{(r)}, \tag{10}$$

with $G^{(k)}$ denoting the cyclic group of integers modulo s_k. Note that $s_1 = s$ and $\prod s_k = |G|$. Putting $c_k = s/s_k$ let us construct the r-vector $\mathbf{b}_0$ and the $r \times n$ matrix B, over the set $S = \{0, 1, \ldots, s-1\}$, as follows:

$$\mathbf{b}_0 = \begin{bmatrix} c_1 h_0^{(1)} \\ c_2 h_0^{(2)} \\ \vdots \\ c_r h_0^{(r)} \end{bmatrix}, \qquad B = \begin{bmatrix} c_1 h_1^{(1)} & c_1 h_2^{(1)} & \cdots & c_1 h_n^{(1)} \\ c_2 h_1^{(2)} & c_2 h_2^{(2)} & \cdots & c_2 h_n^{(2)} \\ \vdots & \vdots & & \vdots \\ c_r h_1^{(r)} & c_r h_2^{(r)} & \cdots & c_r h_n^{(r)} \end{bmatrix}, \tag{11}$$

where $h_i^{(k)}$ stands for the kth component of the element $h_i \in G$ in the representation (10). Let us now define X to be the s-ary group code of length n generated modulo s by the rows of B and consider any vector $\mathbf{e} \in \mathbb{Z}^n$ satisfying $\mathbf{e}B^T \equiv \mathbf{b}_0^T \pmod{s}$. Note that X is isomorphic to G. It appears from (1) that the code C consists of those vectors over A that are $\mathbf{e}$-translates of vectors orthogonal to X modulo s. Thus,

$$C = \bigcap_{\mathbf{x} \in X} \{\mathbf{v} \in A^n : \langle \mathbf{v} - \mathbf{e}, \mathbf{x} \rangle \equiv 0 \pmod{s}\}, \tag{12}$$

with $\langle \mathbf{u}, \mathbf{x} \rangle = u_1 x_1 + \cdots + u_n x_n$. In particular, C_S turns out to be a coset of the *orthogonal complement* X' of X. Indeed, (12) yields $C_S = X' + \mathbf{e}$.

We are now in a position to state a very general theorem about spectral enumerators. Concerning similar results or similar techniques, the reader is especially referred to MacWilliams, Sloane and Goethals (1972) and to

Delsarte (1973, 1978). For any two elements x and y of the group G let us define their inner product $[x, y]$ to be the following integer:

$$[x, y] = \sum_{k=1}^{r} c_k x^{(k)} y^{(k)}, \tag{13}$$

with $c_k = s/s_k$, where $x^{(k)}$ and $y^{(k)}$ are the kth components of x and y, respectively, in the representation (10).

THEOREM 4. *Let ω be a complex primitive sth root of unity. For an alphabet A with s-ary spectrum $\boldsymbol{\theta} = (\theta_0, \theta_1, \ldots, \theta_{s-1})$ and for a check $(n+1)$-tuple $(h_0, \mathbf{h})$, the spectral enumerator $C(\mathbf{z})$ of the code (1) is given by*

$$C(\mathbf{z}) = |G|^{-1} \sum_{x \in G} \omega^{-[x, h_0]} \prod_{i=1}^{n} \left(\sum_{k=0}^{s-1} \theta_k z_k \omega^{k[x, h_i]} \right). \tag{14}$$

Proof. Define Ω to be the Fourier matrix of order s, with (j, k)-entry $\Omega_{j,k} = \omega^{jk}$, for $j, k = 0, 1, \ldots, s-1$. Let us start from the following identities, where $\mathbf{x}$ denotes an arbitrary integer n-tuple:

$$\begin{aligned} ((\boldsymbol{\theta}\mathbf{z})\Omega)^{c(\mathbf{x})} &= \prod_{i=1}^{n} \left(\sum_{k=0}^{s-1} \theta_k z_k \omega^{k x_i} \right) \\ &= \sum_{\mathbf{u} \in S^n} \omega^{\langle \mathbf{u}, \mathbf{x} \rangle} (\boldsymbol{\theta}^{c(\mathbf{u})} \mathbf{z}^{c(\mathbf{u})}) \\ &= \sum_{\mathbf{v} \in A^n} \omega^{\langle \mathbf{v}, \mathbf{x} \rangle} \mathbf{z}^{c(\mathbf{v})}. \end{aligned} \tag{15}$$

(The first expression is immediate; the second one follows by distributivity and by definition of the spectrum $c(\mathbf{u})$; the third one results from the fact that, in view of (2), each vector $\mathbf{u} \in S^n$ with $c(\mathbf{u}) = \boldsymbol{\tau}$ produces $\boldsymbol{\theta}^{\boldsymbol{\tau}}$ vectors $\mathbf{v} \in A^n$ with $c(\mathbf{v}) = \boldsymbol{\tau}$.) Multiplying both members of (15) by $\omega^{-\langle \mathbf{e}, \mathbf{x} \rangle}$ and taking the summation over the code X one obtains

$$\sum_{\mathbf{x} \in X} \omega^{-\langle \mathbf{e}, \mathbf{x} \rangle} ((\boldsymbol{\theta}\mathbf{z})\Omega)^{c(\mathbf{x})} = \sum_{\mathbf{v} \in A^n} \left(\sum_{\mathbf{x} \in X} \omega^{\langle \mathbf{v} - \mathbf{e}, \mathbf{x} \rangle} \right) \mathbf{z}^{c(\mathbf{v})}. \tag{16}$$

Now, in view of (12), the vectors $\mathbf{v}$ of C are characterized by the condition $\langle \mathbf{v} - \mathbf{e}, \mathbf{x} \rangle \equiv 0 \pmod{s}$ for all $\mathbf{x} \in X$. Hence, by a well-known property of the Fourier transform, the sum over X in the right member of (16) equals $|X|$ when $\mathbf{v} \in C$ and otherwise vanishes. As a result, applying definition (8) yields the remarkable identity

$$C(\mathbf{z}) = |X|^{-1} \sum_{\mathbf{x} \in X} \omega^{-\langle \mathbf{e}, \mathbf{x} \rangle} ((\boldsymbol{\theta}\mathbf{z})\Omega)^{c(\mathbf{x})}. \tag{17}$$

The final step of the proof is quite simple. It suffices to make use of the isomorphism between X and G set up by the formula

$$\mathbf{x} = x^{(1)}\mathbf{b}^{(1)} + x^{(2)}\mathbf{b}^{(2)} + \cdots + x^{(r)}\mathbf{b}^{(r)}, \tag{18}$$

where $\mathbf{b}^{(k)}$ stands for the kth row of the matrix B in (11). Then (17) produces the desired expression (14). The details of the verification are left to the reader. ∎

In the rest of this paper we shall apply Theorem 3 to determine the weight enumerator $C(z)$ of certain binary codes mentioned in Section 2. Thus we shall need the particular case $\boldsymbol{\theta} = (1, 1, 0, \ldots, 0)$ of (14), which yields

$$C(z) = |G|^{-1} \sum_{x \in G} \omega^{-[x,h_0]} \prod_{i=1}^{n} (1 + z\omega^{[x,h_i]}). \tag{19}$$

3.1. *Maximum Length Binary 1-Codes*

Most results of this section are not really new (see Section 1). They are presented here mainly to illustrate the theory, without detailed proof. For the sake of simplicity let us first consider the class of binary 1-codes of length $n = s - 1$ introduced by Varshamov and Tenenholtz (1965). By definition, a typical code C in this class consists of the vectors $\mathbf{v} \in \{0, 1\}^n$ that satisfy $v_1 + 2v_2 + \cdots + nv_n \equiv \lambda \pmod{s}$, where λ is a fixed integer. Thus formula (19) reduces to

$$s(1 + z)\, C(z) = \sum_{x=0}^{s-1} \omega^{-\lambda x} \prod_{i=0}^{s-1} (1 + z\omega^{ix}). \tag{20}$$

The i-product in (20) depends only on the greatest common divisor of x and s, denoted by (x, s) in the sequel. In fact, each factor $1 + z\omega^{j(x,s)}$ occurs (x, s) times in this product, for $j = 0, 1, \ldots, d - 1$ with $d = s/(x, s)$. Hence (20) becomes

$$s(1 + z)\, C(z) = \sum_{d \mid s} \left(\sum_{(k,d)=1} \omega^{-\lambda k s/d} \right) \left(\prod_{j=0}^{d-1} (1 + z\omega^{js/d}) \right)^{s/d}. \tag{21}$$

The j-product in (21) obviously equals $1 - (-z)^d$. On the other hand, the k-sum equals $\mu(d_\lambda)\, \phi(d)/\phi(d_\lambda)$ with $d_\lambda = d/(d, \lambda)$, where ϕ stands for the *Euler function* and μ for the *Moebius function*. The argument uses elementary number theory; see, e.g., Vinogradov (1961). As a result one has an explicit formula for the weight enumerator of C, namely

$$s(1 + z)\, C(z) = \sum_{d \mid s} \mu(d_\lambda) \frac{\phi(d)}{\phi(d_\lambda)} (1 - (-z)^d)^{s/d}. \tag{22}$$

Note that $C(z)$ depends only on (λ, s), which is a priori obvious from the remark made in section 2 about isomorphisms. By way of illustration let us give the weight enumerator of all Varshamov–Tenenholtz 1-codes of length 8 (i.e., $s = 9$). For $(\lambda, 9) = 9, 3$ and 1 one has successively

$$C(z) = 1 + 4z^2 + 6z^3 + 8z^4 + 6z^5 + 4z^6 + z^8,$$

$$C(z) = z + 3z^2 + 7z^3 + 7z^4 + 7z^5 + 3z^6 + z^7,$$

$$C(z) = z + 3z^2 + 6z^3 + 8z^4 + 6z^5 + 3z^6 + z^7.$$

Next, let us treat the generalization considered by Constantin and Rao (1979). Here a typical code C consists of the vectors $\mathbf{v} \in \{0, 1\}^n$ that satisfy the check equation $v_1 h_1 + \cdots + v_n h_n = \lambda$, where the h_i's are the distinct nonzero elements of any finite Abelian group G while λ is an arbitrary fixed element of G. Theorem 4 contains an explicit formula for the weight enumerator of C. Although somewhat more complicated, the derivation from (19) is similar to that indicated above in the case of a cyclic group G. The details of the proof are omitted.

THEOREM 4. *Let G be a finite Abelian group of order q and period s. Given a divisor d of s and a divisor k of d, let $\pi(k, d)$ denote the number of elements $x \in G$ of period d satisfying $[x, \lambda] \equiv s/k \pmod{s}$, with the inner product $[\cdot, \cdot]$ defined as in (13). Then the weight enumerator $C(z)$ of the Constantin–Rao code C is given by*

$$q(1+z)\, C(z) = \sum_{d \mid s} \left(\sum_{k \mid d} \mu(d)\, \pi(k, d) \right) (1 - (-z)^d)^{q/d}. \tag{23}$$

Remark. It is obvious that $\pi(k, d)$ vanishes when k does not divide the period of λ. Thus $k \mid d$ can be replaced in (23) by $k \mid (l, d)$ with $l = \text{period}(\lambda)$. In case G is cyclic, $\pi(k, d)$ vanishes for $k \neq d_\lambda$ and equals $\phi(d)/\phi(d_\lambda)$ for $k = d_\lambda$, so that (23) reduces to (22).

As an example let us consider the group G characterized by $r = 2$, $s_1 = p^2$, $s_2 = p$, where p is a prime. It turns out that G has four orbits under the action of its automorphism group. These orbits contain the elements $\lambda = (0, 0)$, $(p, 0)$, $(0, 1)$ and $(1, 0)$, respectively, in the representation (10), and have cardinality 1, $p - 1$, $p(p-1)$ and $p^2(p-1)$, respectively. Computing the values of $\pi(k, d)$ shows that the last two orbits yield the same weight enumerator. The collection of results (23) can be written in matrix notation as follows:

$$p^3(1+z) \begin{bmatrix} C^1(z) \\ C^2(z) \\ C^3(z) \end{bmatrix} = \begin{bmatrix} 1 & p^2 - 1 & p^2(p-1) \\ 1 & p^2 - 1 & -p^2 \\ 1 & -1 & 0 \end{bmatrix} \begin{bmatrix} (1+z)^{p^3} \\ (1-(-z)^p)^{p^2} \\ (1-(-z)^{p^2})^p \end{bmatrix},$$

with $C^1(z)$, $C^2(z)$, $C^3(z)$ denoting the weight enumerator $C(z)$ for the choice $\lambda = (0, 0)$, $(p, 0)$, and $(1, 0)$ or $(1, 0)$, respectively.

The example above shows that $C(z)$ generally depends on λ and not only on $l = \text{period}(\lambda)$ as in the case of cyclic groups, while distinct values of l may yield the same $C(z)$. A general elucidation of this phenomenon resorts to the theory of duality in Schur rings (see Tamaschke (1963) and Delsarte (1973)), and goes beyond the scope of this paper.

Substituting $z = 1$ into (23) leads to a closed form expression for the cardinality $|C| = C(1)$ of the code. It is clear that, for any group G, this cardinality is maximal for the choice $\lambda = 0$. (The result was first proved by Constantin and Rao (1979).) Examining the analytic expression of $|C|$, McEliece and Rodemich (1980) and Helleseth and Kløve (1981) were able to prove the truth of a conjecture made by Constantin and Rao (1979) saying that, for a given order q and for $\lambda = 0$, the largest code C is produced by the group G having the largest number of elementary divisors.

Theorem 4 allows one to identify good constant weight codes with minimum distance four. (The construction is explained at the end of Section 2.) The results thus obtained agree with those given by Graham and Sloane (1980). Since these authors did not consider all possible groups, let us mention an improvement of their results for the length $n' = 24$ in two cases, namely, $|\Gamma_8| = 30789$ and $|\Gamma_{10}| = 112952$, which are produced by the group G with $s_1 = 6$, $s_2 = s_3 = 2$. Let us also give the cardinalities of the largest codes Γ_k for the length $n' = 25$; one obtains $|\Gamma_2| = 12$, $|\Gamma_3| = 92$, $|\Gamma_4| = 506$, $|\Gamma_5| = 2130$, $|\Gamma_6| = 7034$, $|\Gamma_7| = 19228$, $|\Gamma_8| = 43263$, $|\Gamma_9| = 81719$, $|\Gamma_{10}| = 130760$, $|\Gamma_{11}| = 178296$, $|\Gamma_{12}| = 208012$. All these "optimal codes" are produced by the noncyclic group (of order 25) and the choice $\lambda = 0$.

Let us make a final observation about the numerical results of our analysis. For a given order q, the weight distributions of the various codes C are close to each other and close to the normalized binomial distribution. The same comment can be made concerning the codes analysed below.

3.2. *Generalized Varshamov 2-Codes*

The last part of this paper is devoted to binary generalized Varshamov codes as defined in Section 2. Thus a typical code C consists of the vectors $\mathbf{v} \in \{0, 1\}^n$ that satisfy $v_1\alpha_1^k + \cdots + v_n\alpha_n^k = \lambda_k$ for $k = 1,..., t$, where the α_i's are distinct nonzero elements of the field $F = GF(p^m)$ while the λ_k's are arbitrary elements of F.

Let ψ be a homomorphism from the field F onto its prime subfield $S = GF(p)$. When applied to generalized Varshamov codes, (19) becomes

$$p^{mt}C(z) = \sum_{f \in P} \omega^{-\psi((f,\lambda))} \prod_{i=1}^{n} (1 + z\omega^{\psi(f(\alpha_i))}), \tag{24}$$

where P denotes the space of polynomials $f(x) = f_1 x + f_2 x^2 + \cdots + f_t x^t$, with coefficients $f_k \in F$, and $\langle f, \lambda \rangle$ stands for $\Sigma f_k \lambda_k$. From a computational viewpoint, (24) is an efficient formula when t is relatively small. In what follows we shall consider the case of 2-codes with full length and focus attention mainly on prime fields.

Thus let $m = 1$, $t = 2$ and $n = p - 1$ with p an odd prime. For convenience, put $\lambda = \lambda_1$ and $\mu = \lambda_2$. Then (24) immediately yields

$$p^2(1 + z)\, C(z) = \sum_{a,b \in S} \omega^{-a\mu - b\lambda} \prod_{x \in S} (1 + z\omega^{ax^2 + bx}), \tag{25}$$

with $S = \{0, 1, \ldots, p - 1\}$. Let us decompose the summation (25) into several parts. The contribution afforded by $a = b = 0$ obviously is $\Sigma(0, 0) = (1 + z)^p$. Putting $S^* = \{1, 2, \ldots, p - 1\}$ one readily verifies that the contribution of $a = 0$, $b \in S^*$ in (25) equals $\Sigma(0, S^*) = (p\delta_{0,\lambda} - 1)(1 + z^p)$, with the Kronecker δ. Next, let Q and N denote the subsets of S^* consisting of the quadratic and nonquadratic residues (mod p), respectively. Using the identity $ax^2 + bx = a(x + b/2a)^2 - b^2/4a$ one obtains the following expression for the contribution of $a \in Q$, $b \in S$ in (25):

$$\Sigma(Q, S) = \sum_{a \in Q} \sum_{b \in S} \omega^{-a\mu - b\lambda} \left[(1 + z\omega^{-b^2/4a}) \prod_{c \in Q} (1 + z\omega^{c - b^2/4a})^2 \right]. \tag{26}$$

To progress further in the analysis of (26), introduce the polynomial

$$g(z) = (1 + z) \prod_{c \in Q} (1 + z\omega^c)^2 = 1 + z^p + \sum_{k=1}^{p-1} g_k z^k. \tag{27}$$

The coefficients g_k are algebraic integers, which belong to the extension field $\mathbb{Q}[\theta]$ of the rational field $\mathbb{Q}$ by the number

$$\theta = 1 + 2 \sum_{c \in Q} \omega^c = \pm(-1)^{(p-1)/4} p^{1/2}. \tag{28}$$

(See, e.g., Lang (1970).) The factor under square brackets in (26) is $g(z\omega^{-b^2/4a})$. Hence, making use of (27), one obtains

$$\Sigma(Q, S) = (1 + z^p) \sum_{a \in Q} \omega^{-a\mu} \sum_{b \in S} \omega^{-b\lambda} + \sum_{k=1}^{p-1} g_k z^k \left(\sum_{a \in Q} \sum_{b \in S} \omega^{-a\mu - b\lambda - kb^2/4a} \right). \tag{29}$$

The first term in (29) is easily identified; in view of the well-known properties of quadratic residues, this term reduces to

$$\frac{p}{2}(1+z^p)\,\delta_{0,\lambda}(p\delta_{0,\mu}-1+\chi(-\mu)\theta), \tag{30}$$

where $\chi(u)$ is the *quadratic character* (i.e., the Legendre symbol), assuming the value 0, 1 or -1 according as the residue of $u \pmod p$ vanishes, belongs to Q or to N, respectively. Next, let us consider the sum over a and b in the second term of (29), for a fixed value of k. Putting $x = b + 2a\lambda/k$ one deduces the following expressions for the sum in question:

$$\begin{aligned}\sum_{a\in Q}\sum_{x\in S}\omega^{a(-\mu+\lambda^2/k)-kx^2/4a} &= \sum_{a\in Q}\omega^{a(-\mu+\lambda^2/k)}\left(1+2\sum_{c\in Q}\omega^{-kc}\right)\\ &= \tfrac{1}{2}(p\delta_{\mu,\lambda^2/k}-1+\chi(-\mu+\lambda^2/k)\theta)\,\chi(-k)\theta. \end{aligned}\tag{31}$$

This concludes computation of $\Sigma(Q, S)$.

The contribution $\Sigma(N, S)$ afforded to (25) by the elements $a \in N$, $b \in S$ is determined in exactly the same manner as above. The only differences lies in the fact that θ must be replaced by its algebraic conjugate $\bar\theta = -\theta$; thus g_k must be changed into $\bar g_k$. Grouping all terms together, using (30) and (31), one obtains

$$\begin{aligned}p^2(1+z)\,C(z) &= \Sigma(0,0)+\Sigma(0,S^*)+\Sigma(Q,S)+\Sigma(N,S)\\ &= (1+z)^p+(p^2\delta_{0,\lambda}\delta_{0,\mu}-1)(1+z^p)\\ &\quad + p\sum_{k=1}^{p-1}\chi(\lambda^2-k\mu)\,R(g_k)\,z^k\\ &\quad + \sum_{k=1}^{p-1}\chi(-k)(p\delta_{\lambda^2,k\mu}-1)\,R(\theta g_k)\,z^k,\end{aligned}\tag{32}$$

where $R(\xi)$ denotes $(\xi+\bar\xi)/2$ for $\xi \in \mathbb{Q}[\theta]$.

Let us now explain how to determine the coefficients appearing in (32). Define the rational polynomials $a(z)$ and $b(z)$, of formal degree $(p-1)/2$, via the equation

$$f(z) = \prod_{c\in Q}(1+z\omega^c) = a(z)+\theta b(z). \tag{33}$$

(It turns out that $2a(z)$ and $2b(z)$ have integer coefficients.) Now $g(z) = (1+z)\,f^2(z)$, by definition. Hence, using $f(z)\,\bar f(z) = (1+z^p)/(1+z)$, one easily deduces from (33) and (28)

$$\begin{aligned}R(\theta g(z)) &= 2\chi(-1)\,p(1+z)\,a(z)\,b(z),\\ R(g(z)) &= 1+z^p+2\chi(-1)\,p(1+z)\,b^2(z).\end{aligned}\tag{34}$$

Substituting into (32) the values of $R(\theta g_k)$ and $R(g_k)$ resulting from (34) we finally arrive at a rather satisfactory expression for $C(z)$, which we quote as a theorem.

THEOREM 6. *Let x_k and y_k denote the coefficients of z^k in the rational polynomials $(1+z)\,a(z)\,b(z)$ and $(1+z)\,b^2(z)$, respectively, with $a(z)$ and $b(z)$ defined from* (33). *Then the weight enumerator $C(z)$ of the Varshamov binary 2-code of length $n=p-1$, with $\lambda_1=\lambda$ and $\lambda_2=\mu$, is given by*

$$p^2(1+z)\,C(z)=(1+z)^p+(p^2\delta_{0,\lambda}\,\delta_{0,\mu}-1)(1+z^p)-2p\sum_{k=1}^{p-1}\chi(k)\,x_k z^k$$

$$+2p^2\sum_{k=1}^{p-1}(\chi(k\mu-\lambda^2)\,y_k+\delta_{\lambda^2,k\mu}\chi(k)\,x_k)\,z^k. \tag{35}$$

It is interesting to notice that each of the four terms in (35) must be divisible by $1+z$. In particular, for the fourth term this forces

$$x_j=-\sum_{k=1}^{p-1}(-1)^{k-j}\chi(k-j)\,y_k, \qquad 1\leqslant j\leqslant p-1. \tag{36}$$

Consequently, all information needed to compute $C(z)$ by means of (35) is contained in the polynomial $b(z)$. Let us give this for the values $p=17$, 19 and 23, successively:

$$2b(z)=z-z^2+z^3-2z^4+z^5-z^6+z^7,$$
$$2b(z)=z-z^3-z^4+z^5+z^6-z^8,$$
$$2b(z)=z-z^2+z^4-2z^5+2z^6-z^7+z^9-z^{10}.$$

Note that $b(-z)=\chi(-1)\,b(z)$. By way of illustration, let us indicate the cardinalities c of the Varshamov 2-codes of length 16 (with $p=17$) and the numbers $N(c)$ counting the codes of each cardinality.

c:	223	224	226	227	228	230	231
$N(c)$:	8	65	64	16	96	32	8

The small deviation of the c's with respect to the average value given by Theorem 3 is a striking phenomenon. (On the other hand, the small number of distinct c's is readily explained from considering the isomorphisms in the class of Varshamov codes.) In addition, again for $n=16$, let us write down

the weight enumerator of the largest codes (characterized by $\lambda = 0$ and $\mu \in Q$ in this case).

$$C(z) = z^2 + z^{14} + 2(z^3 + z^{13}) + 7(z^4 + z^{12}) + 16(z^5 + z^{11}) + 26(z^6 + z^{10}) + 42(z^7 + z^9) + 43z^8.$$

The reader could check these results by means of (35), using the expression of $b(z)$ given above (for $p = 17$).

It is also possible to derive explicit forms of (24) when $m \geqslant 2$, again for $t = 2$, $p =$ odd prime and $n = p^m - 1$. Let us give the result, without proof, for the case $m = 2$. (The formula hereunder appears to be simpler, from a computational viewpoint, than that of Theorem 6.)

THEOREM 7. *For $k = 0, 1, \ldots, p-1$ let $a_k(\zeta)$ denote the integer polynomial of formal degree $p-1$ defined from the expansion*

$$\left(\frac{1+z^p}{1+z}\right)^p = \sum_{k=0}^{p-1} z^k a_k(z^p). \tag{37}$$

On the other hand, let χ denote the quadratic character in the Galois field $F = GF(p^2)$, defined by $\chi(0) = 0$ and $\chi(u) = 1$ or -1 according as u is a square or a nonsquare in F. The weight enumerator $C(z)$ of the binary generalized Varshamov 2-code C of full length $n = p^2 - 1$, with $\lambda_1 = \lambda$ and $\lambda_2 = \mu$ in F, is given by

$$\begin{aligned} 2p^4(1+z)\,C(z) &= 2(1+z)^{p^2} + (1+z^p)^p(p^2\delta_{0,\lambda}(p^2\delta_{0,\mu} + 1 + p\chi(\mu)) - 2) \\ &\quad + p^2(1+z^p)\,\delta_{0,\lambda}(p^2\delta_{0,\mu} - 1 - p\chi(\mu))\,a_0(z^p) \\ &\quad + p(1+z^p)^{p-1} \sum_{k=1}^{p-1} \binom{p}{k} (p^2\delta_{\lambda^2,k\mu} - 1 + p\chi(k\mu - \lambda^2))\,z^k \\ &\quad - p(1+z^p) \sum_{k=1}^{p-1} (p^2\delta_{\lambda^2,k\mu} - 1 - p\chi(k\mu - \lambda^2))\,z^k a_k(z^p). \end{aligned} \tag{38}$$

The authors have investigated formulas (35) and (38) in order to identify good constant weight codes with minimum distance 6 (see Theorem 2 and final paragraph of Section 2). The numerical values thus obtained check with those given by Graham and Sloane (1980) for lengths $n' \leqslant 24$. As for the case $n' = 25$, not mentioned by these authors, let us give the cardinalities of the largest codes Γ_k deduced from Theorem 7 (with $p = 5$); one has $|\Gamma_3| = 8$, $|\Gamma_4| = 22$, $|\Gamma_5| = 100$, $|\Gamma_6| = 288$, $|\Gamma_7| = 796$, $|\Gamma_8| = 1738$, $|\Gamma_9| = 3299$, $|\Gamma_{10}| = 5360$, $|\Gamma_{11}| = 7152$, $|\Gamma_{12}| = 8323$.

Let us finally mention that, contrarily to the situation in Section 2, the choice of the pair (λ, μ) yielding the largest code C is not evident at all. The

optimal choice (which, in the examples considered, turns out to be unique within isomorphisms) is indicated hereunder, together with the corresponding value of $|C|$, for a few values of the length n.

n:	12	16	18	22	24
(λ, μ):	(1, 0)	(0, 1)	(0, 0)	(1, 2)	(0, 0)
$\|C\|$:	29	231	748	7946	26956

ACKNOWLEDGMENTS

The authors are grateful to R. J. McEliece and to an anonymous referee who called their attention to some useful references.

RECEIVED: December 13, 1979; REVISED: May 7, 1981

REFERENCES

BERLEKAMP, E. R. (1968), "Algebraic Coding Theory," McGraw–Hill, New York.

BOSE, B. AND RAO, T. R. N. (1978), "On the Theory of Unidirectional Error Correcting/Detecting Codes, "Dept. Comp. Sci., Southern Methodist University, Dallas, Texas, Technical Report CS7817.

CONSTANTIN, S. D. AND RAO, T. R. N. (1979), On the theory of binary asymmetric error correcting codes, *Inform. Contr.* **40**, 20–36.

CURTIS, C. W. AND REINER, I. (1962), "Representation Theory of Finite Groups and Associative Algebras," Wiley–Interscience, New York.

DELSARTE, P. (1973), "An Algebraic Approach to the Association Schemes of Coding Theory," Philips Res. Repts Suppl. 10.

DELSARTE, P. (1978), Partial-optimal piecewise decoding of linear codes, *IEEE Trans. Inform. Theory* **IT-24**, 70–75.

GINZBURG, B. D. (1967), A number-theoretic function having application in coding theory, *Problemy Kibernetiki* **19**, 249–252.

GRAHAM, R. L. AND SLOANE, N. J. A. (1980), Lower bounds for constant weight codes, *IEEE Trans. Inform. Theory*, **IT-26**, 37–41.

HELLESETH, T. AND KLØVE, T. (1981), On group theoretic codes for asymmetric channels, *Inform. Contr.*, in press.

LANG, S. (1965), "Algebra," Addison–Wesley, Reading, Mass.

MACWILLIAMS, F. J. (1963), A theorem on the distribution of weights in a systematic code, *Bell System Tech. J.* **42**, 79–94.

MACWILLIAMS, F. J., SLOANE, N. J. A., AND GOETHALS, J. M. (1972), The MacWilliams identities for nonlinear codes, *Bell System Tech. J.* **51**, 803–819.

MAZUR, L. E. (1974), Correcting codes for asymmetric errors, *Problemy Peredachi Informatsii*, **10**, No. 4, 40–46.

MCELIECE, R. J. (1973), A comment on "A class of codes for asymmetric channels and a problem from the additive theory of numbers", *IEEE Trans. Inform. Theory* **IT-19**, 137.

MCELIECE, R. J. AND RODEMICH E. R. (1980), The Constantin–Rao construction for binary asymmetric error-correcting codes, *Inform. Contr.* **44**, 187–196.

NALBANDYAN, M. N. (1974), Note on two classes of nonlinear codes, *Problemy Peredachi Informatsii*, 10, No. 2, 61–63.

RAO, T. R. N. AND CHAWLA, A. S. (1975), Asymmetric error correcting codes for some LSI semiconductor memories, in "The Annual Southeastern Symposium on System Theory," pp. 170–171.

STANLEY, R. P. AND YODER, M. F. (1973), "Study of Varshamov Codes for Asymmetric Channels," Jet Propulsion Laboratory Technical Report 32–1526, Vol. 14, pp. 117–122.

TAMASCHKE, O. (1963), Zur Theorie der Permutationsgruppen mit regulärer Untergruppe, I and II, *Math. Z.* **80**, 328–354 and 443–465.

VARSHAMOV, R. R. (1973), A class of codes for asymmetric channels and a problem from the additive theory of numbers, *IEEE Trans. Inform. Theory*, **IT-19**, 92–95.

VARSHAMOV, R. R. AND TENENHOLTZ G. M. (1965), A code for correcting a single asymmetric error, *Automat. Telemekh.* **26**, No. 2, 288–292.

VINOGRADOV, I. M. (1961), "An Introduction to the Theory of Numbers," Pergamon, Oxford.